



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 7450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,602	07/30/2001	Christopher P. Jalbert	04860P2441	5216

7590 11/15/2005

James C. Sheller  
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP  
Seventh Floor  
12400 Wilshire Boulevard  
Los Angeles, CA 90025-1026

EXAMINER

SCHUBERT, KEVIN R

ART UNIT PAPER NUMBER

2137

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/918,602

Applicant(s)

JALBERT ET AL.

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 17 October 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-41 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-41 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |                                                                                                                                             |                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                                                 | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                                        | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>10172005</u> | 6) <input type="checkbox"/> Other: _____                                                |

### DETAILED ACTION

Claims 1-41 have been considered. The examiner maintains the rejections of the last office action.

5

#### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

10

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

15

Claims 1-6 and 20-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Vogelesang, U.S. Patent No. 5,953,424.

As per claims 1,20,21, and 22, the applicant describes a cryptographic method with the following limitations which are met by Vogelesang:

20

a) generating, at a first entity, a first session key  $K_B$  based on the second public key  $M_A$  (Col 16, lines 39-42);

b) encrypting, at the first entity, a first random nonce  $N_B$  using at least a first password  $P_B$  and a first public key  $M_B$  to obtain an encrypted random nonce, the first public key  $M_B$  and the second public key  $M_A$  being session specific, the first public key  $M_B$  to be used at a second entity to derive the first session key (Col 16, lines 64-67);

25

c) transmitting the encrypted random nonce from the first entity (Col 16, lines 64-67);

d) receiving a response to the encrypted random nonce (Col 17, lines 19-24);

e) authenticating through determining whether the response includes a correct modification of the first random nonce (Col 17, lines 28-30);

Art Unit: 2137

As per claim 2, the applicant describes the method of claim 1, which is met by Vogelesang, with the following limitations which are also met by Vogelesang:

a) generating a first secret  $S_B$  from at least the first password  $P_B$  and the first public key  $M_B$  (Col 16, lines 39-42);

5        b) encrypting the first random nonce  $N_B$  using at least the first secret  $S_B$  (Col 16, lines 64-67);

c) wherein the first secret  $S_B$  and the first session key  $K_B$  are different (Col 16, lines 64-67);

As per claims 3 and 4, the applicant describes the method of claim 2, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

10        Checking whether a received modification of the first random nonce equals a modification of the first random nonce as applied to the first random nonce by the first entity (Col 17, lines 25-37).

As per claim 5, the applicant describes the method of claim 2, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

15        a) generating a first random number  $R_B$  (Col 16, lines 39-40);

b) computing the first session key  $K_B$  from the second public key  $M_A$  raised to the exponential power of the first random number  $R_B$ , modulo a parameter  $B_B$  (Col 16, lines 39-42).

20        As per claim 6, the applicant describes the method of claim 2, which is met by Vogelesang, with the following limitation which is also met by Vogelesang:

Wherein the first secret  $S_B$  is generated using a combining function  $f_B$  on at least the first password  $P_B$  and the first public key  $M_B$  (Col 8, lines 7-10).

25        (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Art Unit: 2137

Claims 1-2,6-10,20-22,24-25,29-31, and 38-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Wu (Wu, Thomas. The Secure Remote Password Protocol. November 11, 1997. Computer Science Department. Stanford University).

- 5           As per claims 1-2,20-22,24-25, and 38-40, the applicant describes a cryptographic method with the following limitations which are met by Wu:
- a) generating, at a first entity, a first session key  $K_B$  based on the second public key  $M_A$  (pages 6-7);
  - b) encrypting, at the first entity, a first random nonce  $N_B$  using at least a first password  $P_B$  and a  
10 first public key  $M_B$  to obtain an encrypted random nonce, the first public key  $M_B$  and the second public key  $M_A$  being session specific, the first public key  $M_B$  to be used at a second entity to derive the first session key (pages 6-7);
  - c) transmitting the encrypted random nonce from the first entity (pages 6-7);
  - d) receiving a response to the encrypted random nonce (pages 6-7);
  - 15 e) authenticating through determining whether the response includes a correct modification of the first random nonce (pages 6-7);

As per claims 6-10 and 29-31, the applicant describes the method of claims 1 and 38, which are met by Wu, with the following limitation which is also met by Wu:

- 20           a) wherein the first secret  $S_B$  is generated using the combining function  $f_B$  on the first password  $P_B$  and the second public key  $M_A$  and the first public key  $M_B$  (pages 6-7).
- (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent  
25 granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.
- 30

Art Unit: 2137

Claims 1-2,6-10,20-22, and 29-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Vanstone, U.S. Patent Application Publication No. 2001/0042205.

As per claims 1,20,21, and 22, the applicant describes a cryptographic method with the following limitations which are met by Vanstone:

a) generating, at a first entity, a first session key  $K_B$  based on the second public key  $M_A$  ([0046]-[0062]);

b) encrypting, at the first entity, a first random nonce  $N_B$  using at least a first password  $P_B$  and a first public key  $M_B$  to obtain an encrypted random nonce, the first public key  $M_B$  and the second public key  $M_A$  being session specific, the first public key  $M_B$  to be used at a second entity to derive the first session key ([0046]-[0062]);

c) transmitting the encrypted random nonce from the first entity ([0046]-[0062]);

d) receiving a response to the encrypted random nonce ([0046]-[0062]);

e) authenticating through determining whether the response includes a correct modification of the first random nonce ([0046]-[0062]);

As per claims 2 and 6, the applicant describes the method of claim 1, which is met by Vanstone, with the following limitations which are also met by Vanstone:

a) generating a first secret  $S_B$  from at least the first password  $P_B$  and the first public key  $M_B$  (Vanstone: [0046]-[0062]);

b) encrypting the first random nonce  $N_B$  using at least the first secret  $S_B$  (Vanstone: [0046]-[0062]);

c) wherein the first secret  $S_B$  and the first session key  $K_B$  are different (Vanstone: [0046]-[0062]).

As per claims 7-10 and 29-31, the applicant describes the method of claims 6,2, and 28, which are met by Vanstone, with the following limitations which are also met by Vanstone:

Art Unit: 2137

a) combining the second public key  $M_A$  and the first public key  $M_B$  with the first password  $P_B$  to produce a first result (Vanstone: [0046]-[0062]);

b) hashing the first result with a secure hash (Vanstone: [0046]-[0062]).

5

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

10

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15

Claims 14-19,24-25,26-27, and 33-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Schneier (Schneier, Bruce. Applied Cryptography. John Wiley & Sons. 1996. Washington DC. Pages 4-5 and 357).

20

As per claims 24 and 38-40, the applicant describes a cryptographic method comprising the following limitations which are met by Vogelesang and Schneier:

a) receiving at a first entity a second public key  $M_A$  and an encrypted second random number (Vogelesang: Col 16, lines 33-38; lines 64-68);

b) generating a first session key  $K_B$  based on the second public key  $M_A$  (Vogelesang: Col 16, lines 39-42);

25

c) decrypting using at least a first password  $P_B$  and the second public key  $M_A$  to retrieve a second random number  $N_A$  from the encrypted second random number (Vogelesang: Col 17, lines 1-18);

d) modifying the second random number  $N_A$  to obtain a modified second random number (Vogelesang: Col 17, lines 19-24);

Art Unit: 2137

e) encrypting the modified second random number using at least the first password  $P_B$  and a first public key  $M_B$  to obtain an encrypted random package (Vogelesang: Col 7, lines 19-24; Schneier: pages 4-5);

f) transmitting the encrypted random package from the first entity (Vogelesang: Col 17, lines 25-27).

Vogelesang discloses all the limitations of the above claim except for encrypting the modified second number at the first entity using a first password **and** a first public key (part e). Vogelesang discloses the use of passwords, such as K and J factors, which are used to construct the shared secret (session key) which is used to encrypt the modified second random number. However, Vogelesang discloses that the session key at the first entity is constructed using a received second public key and a password, not a first public key and a password.

Schneier discloses the idea of public key cryptography in which a message may be encrypted using a recipient's public key so that only the corresponding private key of the recipient may decrypt the message (Schneier: pages 4-5). Schneier also discloses the idea that a message may be doubly encrypted with two keys to enhance security (Schneier: pages 357). Combining the ideas of Schneier into the system allows the modified second number to be encrypted with a first session key as prescribed by Vogelesang and then doubly encrypted with a recipient's public key (ie a first public key) thereby satisfying the limitations of part e. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier with those of Vogelesang to increase security through double encryption.

As per claim 26 and 27, the applicant describes the method of claim 24, which is met by Vogelesang in view of Schneier, with the following limitations which are met by Vogelesang:

- a) generating a first random number  $R_B$  (Col 16, lines 39-40);
- b) computing the first session key  $K_B$  from the second public key  $M_A$  raised to the exponential power of the first random number  $R_B$ , modulo a parameter  $B_B$  (Col 16, lines 39-42).

Art Unit: 2137

As per claims 14-19,25, and 33-37, the applicant describes the method of claims 2 and 24, which are met by Vogelesang in view of Schneier, with the following limitation which is met by Schneier:

a) wherein encrypting the first random nonce  $N_B$  includes superencrypting the first random nonce  $N_B$  (Schneier: page 357);

5

Claims 11-13,17-19,24,26-32,34-37 and 38-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Vanstone, U.S. Patent Application No. 2001/0042205.

As per claims 24 and 38-40, the applicant describes the following limitations which are met by Vogelesang in view of Vanstone:

10

a) receiving at a first entity a second public key  $M_A$  and an encrypted second random number (Vogelesang: Col 16, lines 33-38; lines 64-68);

b) generating a first session key  $K_B$  based on the second public key  $M_A$  (Vogelesang: Col 16, lines 39-42; Vanstone: [0046]-[0062]);

15

c) decrypting using at least a first password  $P_B$  and the second public key  $M_A$  to retrieve a second random number  $N_A$  from the encrypted second random number (Vogelesang: Col 17, lines 1-18);

d) modifying the second random number  $N_A$  to obtain a modified second random number (Vogelesang: Col 17, lines 19-24);

20

e) encrypting the modified second random number using at least the first password  $P_B$  and a first public key  $M_B$  to obtain an encrypted random package (Vogelesang: Col 7, lines 19-24; Vanstone [0046]-[0062]);

f) transmitting the encrypted random package from the first entity (Vogelesang: Col 17, lines 25-27).

25

Vogelesang discloses all the limitations of the claim except the session key generated in Vogelesang's system does not satisfy the limitations of part e. Combining Vanstone with Vogelesang allows for the construction of a different session key which fuses both the first and second public keys and a password and not just one public key and a password as prescribed in the primary reference. It

Art Unit: 2137

would have been obvious to one of ordinary skill in the art to combine the ideas of Vanstone with those of Vogelesang because doing so allows for the construction of a session key which is more secure since it combines the additional knowledge of an extra public key.

5           As per claims 26-28, the applicant describes the method of claim 24, which is met by Vogelesang in view of Vanstone, with the following limitation which is also met by Vanstone:

          Using the combining function  $f_B$  on the first password  $P_B$  and on the second public key  $M_A$  and the first public key  $M_B$  (Vanstone: [0054] and [0055]).

10           As per claims 29-31, the applicant describes the method of claims 28, which is met by Vogelesang in view of Vanstone, with the following limitations which are also met by Vanstone:

          a) combining the second public key  $M_A$  and the first public key  $M_B$  with the first password  $P_B$  to produce a first result (Vanstone: [0046]-[0062]);

          b) hashing the first result with a secure hash (Vanstone: [0046]-[0062]).

15

          As per claims 11 and 32, the applicant describes the method of claims 2 and 27, which are met by Vogelesang in view of Vanstone, with the following limitations which are also met by Vanstone:

          a) combining the first password  $P_B$  and at least one of the second public key  $M_A$  and the first public key  $M_B$  to generate a first combined result (Vanstone: [0060]);

20           b) combining the first combined result and at least one of the second public key  $M_A$ , the first password  $P_B$ , and the first public key  $M_B$  to generate a second combined result (Vanstone: [0060]);

          The first combined result is the creation of the session key, and the second combined result is the hashing function.

25           As per claims 12 and 13, the applicant describes the method of claim 2, which is met by Vogelesang in view of Vanstone, with the following limitation which is also met by Vogelesang:

Art Unit: 2137

Wherein the first random nonce is encrypted using a symmetrical encryption algorithm (Col 16, lines 64-67).

As per claims 17-19 and 34-37, the applicant describes the method of claims 2 and 24, which are met by Vogelesang in view of Vanstone, with the following limitation which is also met by Vogelesang:

- a) generating a first random number  $N_B$  (Vogelesang: Col 13, lines 41-57);
- b) encrypting a combination of the first random number  $N_B$  and the modified second random number (Vogelesang: Col 13, lines 41-57).

The first random number is V, and the modified second random number is N.

As per claim 41, the applicant describes the method of claim 40, which is met by Vogelesang in view of Vanstone, with the following limitation which is also met by Vogelesang:

Wherein the network is a network operating according to a hypertext transfer protocol and the first public key  $M_B$  is transmitted for session key exchange before the encrypted second random number is received (Col 1, lines 12-14; Col 16, lines 25-67).

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang.

As per claim 23, the applicant describes the system of claim 22, which is met by Vogelesang, with the following limitation:

A network operating according to a hypertext transfer protocol and the first public key  $M_B$  is transmitted with the encrypted random nonce for session key exchange (Col 1, lines 12-14);

Vogelesang does not disclose transmitting the first public key  $M_B$  with the encrypted random nonce. The examiner takes official notice that it would have been obvious to one of ordinary skill in the art at the time the invention was filed to transmit a key with a nonce because doing so is more efficient than having to make two separation transmissions for the key and the nonce.

**Response to Arguments**

Applicant's arguments filed 10/17/05 with respect to claim 1 have been fully considered but they are not persuasive. The applicant argues that Vogelesang does not disclose performing limitations a) and b) at the same location. The examiner disagrees. Regarding part a), a first entity generates a session key S. The session key is based on a first public key X and a second public key Y.  $S = Y^{AKJ} \bmod(n) = X^{BKJ} \bmod(n)$ . Hence, the session key is based on a second public key Y.  $S = Y^{AKJ} \bmod(n) = X^{BKJ} \bmod(n)$ . The first participant encrypts a first random nonce, L, with the session key which is a function of a password and a first public key X. The first participant then sends the encrypted random nonce to the second participant who receives it and modifies it for authentication (Col 16, line 64 to Col 17, line 37).

Applicant's arguments with respect to claim 2 have been fully considered but they are not persuasive. The applicant argues that Vogelesang does not show a secret which is different from the session key. The examiner disagrees. Vogelesang discloses a number of values which meet applicant's broadly claimed "secret". For example, ciphertext  $Z_L$  and ciphertext  $Z_m$  meets applicant's claimed "secret".

Applicant's arguments with respect to claims 14-19, 25, and 33-37 have been fully considered but are moot in view of the new grounds of rejection.

Applicant's arguments with respect to claims 7-10 and 29-31 have been fully considered, but they are not persuasive. The applicant argues that x and y of Vanstone do not qualify as public keys. The examiner disagrees. Vanstone discloses values x and y which are transmitted between A and B and used as keys to construct the session key. The examiner finds nothing in applicant's claimed invention that precludes x and y from being public keys.

Art Unit: 2137

Applicant's arguments with respect to claim 18 have been fully considered but they are not persuasive. The applicant argues that the examiner has not indicated what applicant's "string of random bits" corresponds to. The examiner notes that applicant's broad "string of random bits" is met by a number of values, including L and M.

5

Applicant's arguments with regard to claim 24 have been fully considered but they are not persuasive. The applicant argues that claim 24 is not met by Vogelesang in view of Kaufman. The examiner notes that claim 24 was not rejected by Vogelesang in view of Kaufman in the previous action. Therefore, the applicant's arguments are not persuasive.

10

### **Conclusion**

This action is made non-final.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

15

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

20

25

KS

  
**EMMANUEL L. MOISE**  
**SUPERVISORY PATENT EXAMINER**